



Buffer Overflow Vulnerability in liuyueyi/quick-media

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-24807
State	PUBLISHED
Assigner	GovTech CSG
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-27 09:15:50 UTC
Updated	2026-05-06 17:16:22 UTC
Description	Improper Verification of Cryptographic Signature vulnerability in liuyueyi quick-media (plugins/svg-plugin/batik-codec-fix/src/

Risk And Classification

Primary CVSS: v4.0 5.3 MEDIUM from cve_disclosure@tech.gov.sg

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:N/AU:Y/R:U/V:C/RE:M/U:Amber

Problem Types: CWE-347 | CWE-347 CWE-347 Improper Verification of Cryptographic Signature

Version	Source	Type	Score	Severity	Vector
4.0	cve_disclosure@tech.gov.sg	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:L/SC:N/SI:N/S
4.0	CNA	CVSS	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:L/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

None

None

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:N/AU:Y/R:U/V:C/RE:M/U:Amber

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Liuyueyi	Quick-media	affected v1.0 git	Not specified

References

Reference	Source	Link	Tags
github.com/liuyueyi/quick-media/pull/123	af854a3a-2127-422b-91ae-364da2661108	github.com	
github.com/liuyueyi/quick-media/pull/123	cve_disclosure@tech.gov.sg	github.com	
github.com/css4j/echosvg/discussions/137	af854a3a-2127-422b-91ae-364da2661108	github.com	
github.com/github/advisory-database/pull/7438	af854a3a-2127-422b-91ae-364da2661108	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: TITAN Team (titancaproject@gmail.com) (en)

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report